UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/080,865	02/21/2002	Ross W. Callon	JNP-0159	9630

44987 7590 03/22/2007

HARRITY SNYDER, LLP
11350 Random Hills Road
SUITE 600
FAIRFAX, VA 22030

EXAMINER	
NGUYEN, THANH T	
ART UNIT	**PAPER NUMBER**
2144	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
2 MONTHS	03/22/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/080,865
Filing Date: February 21, 2002
Appellant(s): CALLON, ROSS W.

Glenn Snyder
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed November 27, 2006 appealing from the Office action mailed May 23, 2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

US 2002/0032854 A1 Chen et al (March 14, 2002)

US 2002/0202819 A1 GoldStone (August 1, 2002)

6,560,654 FEDYK 6,560,654

us 2002/0016926 A1 Nguyen et al (February 7, 2002)

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351 (a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 61-62 and 64 are rejected under 35 U.S.C. 102(e) as being anticipated by US 2002/0032854 by Chen et al.

In claim 61, Chen teaches about a method for responding to an attack, comprising: receiving attack information at a central management system (Fig 2, 101) from a first device via a network (Fig 2, 113) (Paragraph 54, lines 1-9); managing a response to the attack at the central management system (Paragraph 45, lines 1-24). Receiving at the central management system, additional attack information from other devices (Fig 2, 106, 107, 109) via the network

(Paragraph 45, lines 1-24); and Communicating by the central management system, information associated with the additional attack information to the first device (Paragraph 45, lines 1-24).

In claim 62, Chen teaches about a method of claim 61, wherein the managing includes: sending the attack information to other devices via a network (Paragraph 45, lines I-24).

In claim 64, Chen teaches about a method of claim 61, wherein the managing includes: collecting information related to the attack information (Paragraph 47, lines 1-11).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-6, 9-15, 17-18, 20-29, 32-38, 40-43, 45-48 and 50-51 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Application Publication No. 2002/0101819 by Goldstone in view of US Patent No. 6560,654 by Fedyk et al.

In claim 1, Goldstone teaches about a system for detecting and responding to an attack, comprising (Fig 4):

a second device " ISP Router (50)" configured to receive the attack information and detect particular traffic based on the attack information (Paragraph 42, lines 1-12);

a first device "firewall (20)" attached to a network and configured to detect an attack based on received traffic, create attack information and forward the attack information to the network (Paragraph 42, lines 1-12);

but does not explicitly teach about using a link state routing protocol or a path vector routing protocol to forward the attack information.

The success of Goldstone invention in reducing DOS attack, relies on a router using a router protocol to inform other routers that an attack has occurred (Paragraph 0024, line 1Paragraph 0028, line 4).

Fedyk teaches about layer three networking (router layer) and the advantage of using the link state routing protocol to rapidly pass on routing information to other routers in a network (Col 1, lines 25-40).

In an DOS attack as in the case of Goldstone it is important that the source of the attack is disable as soon as possible to prevent network failure occurred (Paragraph 0001, line 1Paragraph 0002, line 18).

It would have been obvious for some one of ordinary skill at the time of the invention to improve on Goldstone invention by using the link state routing protocol method of Fedyk in order to provide a rapid response to DOS attack and thus reduce the time taken to recover from the attack.

In claim 2, Goldstone combined with Fedyk, teaches about a system of claim 1, wherein the first device comprises a firewall filter (Gold Para 42, lines 1-12).

`In claim 3, Goldstone combined with Fedyk, teaches about a system of claim t, wherein the first device comprises:

a filter device configured to perform stateful filtering (Gold Para 12, lines 1-17) (Gold Para 20, lines 1-7) (Gold Para 42, lines 1-12).

In claim 4, Goldstone combined with Fedyk, teaches about a system of claim 1, wherein the first device comprises:

a packet generating element configured to generate a link state routing packet that includes the attack information (Gold Para 2, lines 1-7) (Gold Para 42, lines 1-12) (Covered In Claim 1).

In claim 5, Goldstone combined with Fedyk, teaches about a system of claim 1, wherein the second device comprises a router (Gold Para 42, lines 1-12).

In claim 6, Goldstone combined with Fedyk, teaches about a system of claim 1, wherein the first device forwards the attack information using a path vector routing packet (Gold Para 43, lines 1-11). This is the distance method used in Goldstone

In claim 9, Goldstone combined with Fedyk, teaches about a system of claim 1, wherein the second device forwards the attack information to other devices (Fig 4, 130) (Gold Para 42, lines 1-12) (Gold Para 44, lines 1-7).

In claim 10, Goldstone combined with Fedyk, teaches about a system of claim 1, wherein the second device configures a filter based on the attack information (Gold Para 42, lines 1-12) (Gold Para 43, lines 1-11). (router access list is used to realize the filter)

In claim 11, Goldstone combined with Fedyk, teaches about a system of claim 1, wherein the second device uses the attack information for a predetermined amount of time (Gold Para 46, lines 1-8).

In claim 12, Goldstone combined with Fedyk, teaches about a system of claim 1, wherein the second device rate limits the particular traffic (Gold Para 45, lines 1-16).

In claim 13, Goldstone combined with Fedyk, teaches about a system of claim 1, wherein the second device counts the particular traffic (Gold Para 29, lines 1-6). (To determine that a DOS attack has ended, there has to be a reduction in the amount of ill accesses, which cannot be done without a counting function).

In claim 14, Goldstone combined with Fedyk, teaches about a method of detecting and responding to an attack, comprising (Fig 4): detecting an attack at a first device based on incoming traffic (Gold Para 42, lines 1-12); generating attack information defining characteristics of the attack (Gold Para 42, lines 112); sending the attack information to a second device in a network using a link state routing packet or a path vector routing packet (Gold Para 42, lines 1-12) (Covered In Claim 1); detecting traffic at the second device based on the attack information (Gold Para 42, lines 1-12).

In claim 15, Goldstone combined with Fedyk, teaches about a method of claim 14, including: configuring the first device to detect traffic based on the detected attack (Gold Para 42, lines 1-12).

In claim 17, Goldstone combined with Fedyk, teaches about a method of claim 14, wherein the sending includes:

sending the attack information using a distributed routing protocol (Gold Para 43, lines 111).

In claim 18, Goldstone combined with Fedyk, teaches about a method of claim 14, wherein the sending includes:

Sending the attack information using a link state routing protocol (Covered in claim 1).

In claim 20, Goldstone combined with Fedyk, teaches about a method of claim 14, further including:

sending the attack information from the second device to another device (Fig 4,130) (Gold Para 42, lines 1-12).

In claim 21, Goldstone combined with Fedyk, teaches about a method of claim 14, further including:

monitoring the attack at the second device (Gold Para 43, lines 1-11). (The blocking process is done by monitoring for the attacker IP address.)

In claim 22, Goldstone combined with Fedyk, teaches about a method of claim 14, further including:

detecting traffic based on the attack information for a particular period of time (Gold Para 46, lines 1-8).

In claim 23, Goldstone combined with Fedyk, teaches about a method of claim 14, further including: rate limiting traffic that matches attack characteristics defined in the attack information (Gold Para 45, lines 1-16).

In claim 24, Goldstone combined with Fedyk, teaches about a method of claim 14, wherein the sending includes:

sending the attack information using one of a markup language or hypertext protocol (Gold Para 1, lines 1-7).

In claim 25, Goldstone combined with Fedyk, teaches about a device for detecting an attack, comprising (Fig 4, 20):

an attack detection element configured to detect an attack in incoming traffic (Gold Para 42, lines 1-12);

an attack information generator (function that update access list) configured to generate attack information defining characteristics of the attack (Gold Para 12, lines 1-16) (Gold Para 42, lines 1-12); and

a transmitting element configured to transmit the attack information to a device on a network using a link state routing protocol or a path vector routing protocol (Gold Para 42, lines 1-12) (Covered In Claim 1).

In claim 26, Goldstone combined with Fedyk, teaches about a device of claim 25, further comprising: a filter element configured to filter incoming traffic and forward filter information to the attack detection element (Gold Para 20, lines 1-7) (Gold Para 42, lines 1-12).

In claim 27, Goldstone combined with Fedyk, teaches about a device of claim 26, wherein the attack information generator is further configured to send attack information to the filter element (Gold Para 42, lines 1-12).

In claim 28, Goldstone combined with Fedyk, teaches about a device of claim 25, wherein the transmitting element is further configured to transmit the attack information using a distributed routing protocol (Gold Para 43, lines 1-11).

In claim 29, Goldstone combined with Fedyk, teaches about a device of claim 25, wherein the transmitting element is configured to transmit the attack information using a link state routing protocol (Covered in claim 1).

In claim 32, Goldstone combined with Fedyk, teaches about a device of claim 25, wherein the attack is a denial of service attack (Gold Para 25, lines 1-5).

In claim 33, Goldstone combined with Fedyk, teaches about a method of detecting an attack, comprising (Gold Para 42, lines 1-12):

monitoring incoming traffic at a first device to detect an attack (Gold Para 42, lines 1-12); generating attack information defining characteristics of the attack (Gold Para 42, lines 112); and transmitting the attack information to a second device via a network using a link state routing protocol, a path vector routing protocol a markup language protocol or hypertext protocol (Gold Para 42, lines 1-12) (Covered In Claim 1).

In claim 34, Goldstone combined with Fedyk, teaches about a method of claim 33, wherein the attack is a denial of service attack (Gold Para 25, lines 1-5).

In claim 35, Goldstone combined with Fedyk, teaches about a method of claim 33, wherein the monitoring includes:

using information from a filter to detect the attack (Gold Para 19, lines 1-1,0) (Gold Para 42, lines 1-12).

In claim 36, Goldstone combined with Fedyk, teaches about a method of claim 33, wherein the generating includes:

sending attack information to a filter for configuring the filter based on the attack (Gold Para 19, lines 1-10) (Gold Para 41, lines 8-14).

In claim 37, Goldstone combined with Fedyk, teaches about a method of claim 33, further including:

performing stateful filtering on incoming traffic (Gold Para 12, lines 1-17) (Gold Para 20, lines 1-7) (Gold Para 42, lines 1-12).

In claim 38, Goldstone combined with Fedyk, teaches about a method of claim 33, wherein the transmitting includes:

sending the attack information in a packet (Gold Para 2, lines 1-6) (Gold Para 42, lines 1-12).

In claim 40, Goldstone combined with Fedyk, teaches about a method of claim 33, wherein the transmitting includes:

Sending the attack information using a link state routing protocol (Covered in claim 1).

In claim 41, Goldstone combined with Fedyk, teaches about a method of claim 33, wherein the transmitting includes:

sending the attack information using a markup language protocol or a hypertext protocol (Gold Para 1, lines 1-7).

In claim 42, The method of claim 33, wherein the transmitting includes:

sending the attack information in a secure format in claim 43, Goldstone combined with Fedyk, teaches about a device for responding to an attack, comprising: a receiver configured to receive attack information from a first device that sent the attack information (Gold Para 42, lines 1-12); a configuration element configured to configure a second device based on the received attack information (Gold Para 42, lines 1-12); and a transmitting element for transmitting the attack information to another using a link state routing protocol, a path vector routing protocol a markup language protocol or hypertext protocol (Gold Para 42, lines 1-12) (Covered In Claim 1).

In claim 45, Goldstone combined with Fedyk, teaches about a device of claim 43, wherein the configuration element comprises: a filter (Gold Para 20, lines 1-7) (Gold Para 41, lines 8-14); and an attack configuration generator (Gold Para 42, lines 1-12).

In claim 46, Goldstone combined with Fedyk, teaches about a device of claim 43, wherein the configuration element is further configured to configure the second device based on filter information (Gold Para 42, lines 1-12) (Gold Para 43, lines 1-11).

In claim 47, Goldstone combined with Fedyk, teaches about a device of claim 43, wherein the configuration element is further configured to unconfigure the second device after a predetermined period of time after configuring based on the attack information (Gold Para 46, lines 1-8).

In claim 48, Goldstone combined with Fedyk, teaches about a device of claim 43, wherein the second device comprises a router (Gold Para 42, lines 1-12).

In claim 50, Goldstone combined with Fedyk, teaches about a device of claim 43, wherein the configuration element is further configured to detect particular traffic based on the attack information (Gold Para 19, lines 1-11) (Gold Para 41, lines 8-14).

In claim 51, Goldstone combined with Fedyk, teaches about a device of claim 43, wherein the configuration element is further configured to monitor traffic and send monitoring results to the first device (Gold Para 19, lines 1=11) (Gold Para 41, lines 8-14).

Goldstone combined with Fedyk, teaches about the problem of being attack by a malicious attacker and the need to communicate information about the attack to upstream routers (abstract).

Goldstone teaches about the problem of malicious person having access to machine in which attacks are launched (Gold Para 0002, lines 1-17) Nguyen teaches about an improve method of communication between routers using tunneling which prevent unauthorized access (Paragraph 63, lines 1-14) (Paragraph 96, lines 1-12).

When under the scenario of being attack, it is crucial that the information being used to support the recovery be protected from the attacker. The encryption approach of Nguyen guarantees that the information that is exchange between the different entities is only between authorized entities.

It would have been obvious for some one of ordinary skill at the time of the invention to improve on the method of Goldstone and Fedyk by using the encryption scheme of Khosravi to insure that the information that is being transmitted to recovery from an attack is from an authorized source and not the attacker.

Claims 19, 30-31 and 49 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Application Publication No. 2002/0101819 by Goldstone and US Patent No. 6560,654 by Fedyk et al in view of US Patent Application Publication No. 2002/0016926 by Nguyen et al.

(10) Response to Argument

- Appellant argues that Chen does not disclose "*receiving at the central management system, additional attack information from other devices and communicating information associated with the additional attack information to the first device*".

Examiner respectfully disagrees. Applicant argument is vague. Chen discloses receiving at the central management system, additional attack information from other devices and communicating information associated with the additional attack information to the first device as shown in fig.2, and paragraph 0045 (*when the attack on the server 101 from the hosts 113, 114, 116, and 117 of the DDoS attackers has ended, the mobile packet filtering programs installed on the routers 106, 107, 109, and 110 send the history log of the attack to the original mobile packet filtering program installed on the edge router 102 and delete themselves from the routers 106, 107, 109, and 110*).

- Appellant argues that "*neither Goldstone nor Fedyk disclose using a link state routing protocol or a path vector routing protocol to forward attack information*".

Examiner respectfully disagrees. Applicant argument is vague. Fedyk discloses using a link state routing protocol as shown in col.1, lines 25-35 (*link state routing protocols and MPLS can be implemented across a link state routing network*).

- Appellant argues that motivation does not satisfy the requirement to combine Goldstone and Fedyk references.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, It would have been obvious to one of ordinary skill in the art at the time of the invention was made to implement the teachings of Fedyk into the computer system of Goldstone invention to have using the link state routing protocol in order to provide a rapid response to DOS attack and thus reduce the time take to recover from the attack.

- Appellant argues that these two reference absent impermissible hindsight in an attempt to reconstruct application invention.

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

- Appellant argues that Goldstone does not disclose "the firewall filter".

Examiner respectfully disagrees. Applicant argument is vague. Chen discloses the firewall filter as shown in paragraph 0042, lines 1-12. However, Examiner does not see anywhere in claim 2 stated that " is able to forward attack information using a link routing protocol or a path vector routing protocol" as appellant argument in beginning of page 12.

- Appellant argues that motivation does not satisfy the requirement to combine Goldstone, Fedyk and Nguyen references.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, It would have been obvious to one of ordinary skill in the art at the time of the invention was made to implement the teachings of Nguyen into the computer system of Goldstone invention to ensure that the information that is being transmitted to recovery form an attack is from an authorized source and not the attacker.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Examiner
TTN
Art Unit 2144

Conferees:

***

WILLIAM VAUGHN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100